

Serial No. 09/727,313
Attorney Docket No. 020533.0345 (2001P21474US)

Amendments To the Claims:

Please amend the claims as shown. Applicants reserve the right to pursue any cancelled claims at a later date.

1.-30. (Canceled)

31. (Currently Amended) A method of communicating information, comprising:

at a first client, forming a first message by encapsulating a point-to-point data unit within a network address request header, wherein the point-to-point data unit comprises a header including an identifier associated with a second client and a payload comprising information to be communicated to the second client, and wherein the first client comprises a client protocol stack to generate the point-to-point data unit;

at a tunneling server, receiving the first message, removing the network address request header, and encapsulating the point-to-point data unit within a network address response header to form a second message, wherein the tunneling server comprises a server protocol stack to process at least a portion of the first message; and communicating the second message toward the second client.

32. (Original) The method of Claim 31, wherein the network address request header comprises a Dynamic Host Configuration Protocol DISCOVER header or a Bootstrap Protocol REQUEST header.

33. (Original) The method of Claim 31, wherein the network address response header comprises a Dynamic Host Configuration Protocol OFFER header or a Bootstrap Protocol RESPONSE header.

34. (Previously Presented) The method of Claim 31, wherein the point-to-point data unit is encapsulated within a tunneling header prior to being encapsulated into the network address request header, the tunneling header operable to facilitate maintenance of a tunneling session between the tunneling server and the first client.

BEST AVAILABLE COPY

Serial No. 09/727,313
Attorney Docket No. 028333.0345 (2001P21474US)

35. (Original) The method of Claim 34, wherein the tunneling header comprises a tunneling header selected from the group consisting of a Layer Two Tunneling Protocol (L2TP) header, a Point to Point Tunneling Protocol (PPTP), or a Layer Two Forwarding (L2F) header.

36. (Currently Amended) A method of communicating in an enterprise network, comprising:

at a tunneling server, receiving from a first client a first message, the first message formed by encapsulating a point-to-point data unit within a network address request header, the point-to-point data unit comprising a first header that includes an identifier associated with a second client, and a payload comprising information to be communicated to the second client, wherein the tunneling server comprises a protocol stack to process at least a portion of the first message;

encapsulating the first message within a network address response header to form a second message; and
communicating the second message toward the second client.

37. (Original) The method of Claim 36, wherein the network address request header comprises a Dynamic Host Configuration Protocol DISCOVER header or a Bootstrap Protocol REQUEST header.

38. (Original) The method of Claim 36, wherein the network address response header comprises a Dynamic Host Configuration Protocol OFFER header or a Bootstrap Protocol RESPONSE header.

39. (Previously Presented) The method of Claim 36, wherein the point-to-point data unit is encapsulated within a tunneling header, the tunneling header operable to facilitate maintenance of a tunneling session between the tunneling server and the first client.

BEST AVAILABLE COPY

Serial No. 09/727,313
Attorney Docket No. 020533.0345 (2001P21474US)

40. (Original) The method of Claim 39, wherein the tunneling header comprises a tunneling header selected from the group consisting of a Layer Two Tunneling Protocol (L2TP) header, a Point to Point Tunneling Protocol (PPTP), or a Layer Two Forwarding (L2F) header.

41. (Previously Presented) The method of Claim 36, wherein the point-to-point data unit is encapsulated within a tunneling header, the tunneling header operable to facilitate maintenance of a tunneling session between the tunneling server and the second client.

42. (Previously Presented) The method of Claim 36, wherein communicating the second message toward the second client comprises communicating the second message toward a router operable to relay the second message toward the second client without referencing a routing table indexed by data channel addresses.

43. (Original) The method of Claim 42, wherein the identifier comprises a control channel address identifying the second client, the control channel address being different than any data channel address recognized by the router.

44. (Original) The method of Claim 36, wherein the identifier comprises an identifier of the second client other than a control channel address, and further comprising accessing a memory to determine, based on the identifier, a control channel address of the second client.

45. (Previously Presented) The method of Claim 36, wherein the point-to-point data unit comprises information to be applied to an application residing at the second client.

46. (Original) The method of Claim 45, wherein the application residing at the second client comprises a maintenance application operable to diagnose operational characteristics of the second client.

47. (Previously Presented) The method of Claim 36, wherein the point-to-point data unit comprises at least a portion of an application to be installed on the second client.

BEST AVAILABLE COPY

Serial No. 09/727,313
Attorney Docket No. 020533.0345 (2001P21474US)

48. (Previously Presented) The method of Claim 36, further comprising removing the network address request header before encapsulating the first message within the network address response header.

49. (Currently Amended) A computer readable medium operable to execute the following steps on a processor of a computer:

at a tunneling server, receiving from a first client a first message formed by encapsulating a point-to-point data unit within a network address request header, the point-to-point data unit comprising a first header that includes an identifier associated with a second client, and a payload comprising information to be communicated to the second client, wherein the tunneling server comprises a protocol stack to process at least a portion of the point-to-point data unit;

removing the point-to-point data unit from the first message;

encapsulating the point-to-point data unit within a network address response header to form a second message; and

communicating the second message toward the second client.

50. (Previously Presented) The computer readable medium of Claim 49, wherein the point-to-point data unit is encapsulated within a tunneling header, the tunneling header operable to facilitate maintenance of a tunneling session between the tunneling server and the first client.

51. (Previously Presented) The computer readable medium of Claim 49, wherein the point-to-point data unit is encapsulated within a tunneling header, the tunneling header operable to facilitate maintenance of a tunneling session between the tunneling server and the second client.

52. (Previously Presented) The computer readable medium of Claim 49, wherein communicating the second message toward the second client comprises communicating the toward a router operable to relay the second message to the second client without referencing a routing table indexed by data channel addresses.

BEST AVAILABLE COPY

Serial No. 09/727,313
Attorney Docket No. 020533.0345 (2001P21474US)

53. (Previously Presented) The computer readable medium of Claim 52, wherein the point-to-point data unit comprises a control channel address identifying the second client, the control channel address being different than any data channel address recognized by the router.

54. (Original) The computer readable medium of Claim 49, wherein the first identifier comprises an identifier other than a control channel address of the second client, and further comprising accessing a memory to determine, based on the identifier, a control channel address of the second client.

55. (Previously Presented) The computer readable medium of Claim 49, wherein the point-to-point data unit comprises information to be applied to an application residing at the destination client.

56. (Previously Presented) The computer readable medium of Claim 49, wherein the point-to-point data unit comprises at least a portion of an application to be installed on the second client.

57. (Canceled)

58. (Previously Presented) In an enterprise network comprising at least one client coupled to a tunneling server, a tunneling server comprising:

a tunneling module operable to receive a first message formed by encapsulating a point-to-point data unit within a network address request header, and

a protocol stack operable to process at least a portion of the point-to-point data unit to identify a control channel address associated with a destination client;

wherein the tunneling module is further operable to encapsulate the point-to-point data unit within a network address response header to form a second message and wherein the tunneling server is operable to communicate the second message toward the destination client.

BEST AVAILABLE COPY

Serial No. 09/727,313
Attorney Docket No. 020533.0345 (2001P21474US)

59. (Original) The tunneling server of Claim 58, wherein the network address request header comprises a Dynamic Host Configuration Protocol DISCOVER header or a Bootstrap Protocol REQUEST header.

60. (Original) The tunneling server of Claim 58, wherein the network address response header comprises a Dynamic Host Configuration Protocol OFFER header or a Bootstrap Protocol response header.

61. (Previously Presented) The tunneling server of Claim 58, wherein the point-to-point data unit comprises a control channel address identifying the destination client, and wherein the tunneling server is further operable to communicate the first message toward a router for forwarding to the destination client without reference to a routing table indexed by data channel addresses.

62. (Previously Presented) The tunneling server of Claim 58, wherein the point-to-point data unit is encapsulated within a tunneling header and further encapsulated within the network address request header, and wherein the tunneling module is operable to process the tunneling header to maintain a tunneling session between the tunneling server and a client originating the first message.

63. (Original) The tunneling server of Claim 62, wherein the tunneling header comprises a tunneling header selected from the group consisting of a Layer Two Tunneling Protocol (L2TP) header, a Point to Point Tunneling Protocol (PPTP), or a Layer Two Forwarding (L2F) header.

64. (Previously Presented) The tunneling server of Claim 58, wherein the tunneling module is operable to encapsulate the point-to-point data unit within a tunneling header before encapsulating the point-to-point data unit within the network address response header, the tunneling header operable to facilitate maintenance of a tunneling session between the tunneling server and the destination client.

BEST AVAILABLE COPY

Serial No. 09/727,313
Attorney Docket No. 020533.0345 (2001P21474US)

65. (Previously Presented) The tunneling server of Claim 58, wherein the point-to-point data unit comprises a payload comprising information to be applied to an application residing at the destination client.

66. (Original) The tunneling server of Claim 65, wherein the payload comprises information to be applied to a maintenance application residing at the destination client and operable to diagnose operational characteristics of the destination client.

67. (Currently Amended) A system operable to facilitate communication with a destination client in an enterprise network, the system comprising:

a first client comprising:

a client protocol stack operable to generate a point-to-point data unit; and

a tunneling module operable to encapsulate the point-to-point data unit within a network address request header to form a first message;

wherein the first client is operable to communicate the first message toward a tunneling server; and

a tunneling server comprising:

a tunneling module operable to receive the first message; and

a server protocol stack operable to process at least a portion of the point-to-point data unit to identify a control channel address associated with a destination client;

wherein the tunneling module is further operable to encapsulate the point-to-point data unit within a network address response header to form a second message and wherein the tunneling server is operable to communicate the second message toward the destination client.

REST AVAILABLE COPY